



Communications and Information

ELECTRONIC MAIL MANAGEMENT AND USE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available electronically on the USTRANSCOM electronic library.

RELEASABILITY: There are no releasability restrictions on this publication

OPR: TCJ6-OM

Approved By: TCCS (MG Gregory Couch, USA)

Supersedes: USTRANSCOMI 33-30, 9 April 2007

Pages: 13

Distribution: e-Publishing

This instruction establishes policies and procedures for use of electronic mail (e-mail) in the United States Transportation Command (USTRANSCOM). Rules, standards, and guidance for administration and use of e-mail apply to all USTRANSCOM and Joint Enabling Capabilities Command (JECC) military (active duty and reserve), civilians, and contractor personnel regardless of the classification of the information transmitted or received. Throughout this document, all references to USTRANSCOM members also include JECC personnel. Failure to observe the prohibitions and mandatory provisions of this instruction as provided in subparagraphs 2.2.1. through 2.2.6. by military personnel is a violation of the *Uniform Code of Military Justice*, Article 92, Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. The use of a name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by USTRANSCOM. Refer recommended changes and questions about this instruction to the office of primary responsibility using Air Force Form 847, *Recommendation for Change of Publication*. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with USTRANSCOM Instruction 33-32, *USTRANSCOM Records Management Program*.

SUMMARY OF REVISIONS

This document revises policy and procedures for e-mail use in USTRANSCOM to ensure compliance with applicable guidelines. It redefines staff responsibilities and expands the section covering Special Handling Requirements to include the course of action for establishing e-mail digital signatures in the command.

1. References and Supporting Information. References, related publications, abbreviations, acronyms, and terms used in this instruction are listed in Attachment 1.

2. E-mail Policy.

2.1. General. E-mail is used to supplement or replace traditional mail, facsimile, telephone, and other messaging systems. In the context of this instruction, e-mail and electronic messaging are considered synonymous. USTRANSCOM members use government communications systems with the understanding that any type of use may be monitored. By using these systems, the member consents to monitoring.

2.2. USTRANSCOM members may use a government-provided e-mail communications system only for official or authorized uses. Official use includes communications, including emergency communications, that USTRANSCOM has determined necessary in the interests of the Federal Government. Official use includes, when approved by the Commander or a theater commander in the interest of morale and welfare, those communications by USTRANSCOM members who are deployed for extended periods away from home on official business. The following do not constitute official use of government communications systems and are prohibited:

2.2.1. Distributing copyrighted materials by e-mail or e-mail attachments without consent from the copyright owner (failure to obtain consent may violate federal or other law and could subject the individual to civil liability or criminal prosecution).

2.2.2. Sending or receiving e-mail for commercial or personal financial gain using government systems.

2.2.3. Intentionally or unlawfully misrepresenting your identity or affiliation in e-mail communications.

2.2.4. Sending harassing, intimidating, abusive, or offensive material to, or about, others.

2.2.5. Using someone else's identity without proper authority.

2.2.6. Causing congestion on the network by such things as the propagation of chain letters, broadcasting inappropriate messages to groups or individuals, or excessive use of the data storage space on the e-mail host server.

2.3. Authorized personal use, when authorized by a USTRANSCOM designee (a USTRANSCOM designee is the first supervisor in the command who is a commissioned officer or a government civilian holding a grade of General Schedule-11 or above), may include, by way of example and not in limitation, brief communications made while traveling on official business to notify family members of official transportation or schedule changes, or exchanging important time-sensitive information with a spouse or other family members. A USTRANSCOM designee may authorize limited personal use of government-provided e-mail communication, when it:

2.3.1. Serves a legitimate public interest.

2.3.2. Conforms with USTRANSCOM policies.

2.3.3. Does not adversely affect the performance of official duties.

2.3.4. Is of reasonable duration and frequency and, whenever possible, is made during personal time (such as after-duty hours or lunch time).

2.3.5. Does not create significant additional cost to the Department of Defense (DOD) or USTRANSCOM.

2.3.6. Does not reflect adversely on DOD or USTRANSCOM (such as uses involving pornography, chain letters, unofficial advertising, soliciting and selling, violation of statute or regulation, inappropriately handled classified information, or other uses that are incompatible with public service.)

2.4. Authorized usages of the government provided e-mail communication systems described in paragraph 2.3. should be consistent with the requirements of the DOD 5500-7-R, *Joint Ethics Regulation*.

2.5. Auto Forwarding. For operations security reasons, USTRANSCOM members may not auto-forward e-mail to commercial Internet Service Providers. Members using government-owned wireless e-mail devices (e.g., Blackberry) are the only exception.

2.6. Efficient use of bandwidth. The following guidelines apply:

2.6.1. Graphic intensive briefings and other large files should not be sent as e-mail attachments, unless absolutely necessary. Instead, save file on SharePoint or a common drive and e-mail the link. When large attachments must be sent via e-mail, the attachment should be compressed to the maximum extent possible.

2.6.2. Limit usage of the "Reply to All" feature to situations where all original addressees need to receive your individual response.

2.6.3. Do not routinely use the "Return Receipt" e-mail feature. Use only on official e-mail when receipt must be positively verified (e.g., where the e-mail has a direct bearing on the mission).

2.6.4. Official e-mail communications will not contain bandwidth intensive logos, graphics, digital images, cliparts, etc., in the signature block or body of the e-mail unless required as part of the e-mail content.

2.7. Organizational E-mail.

2.7.1. USTRANSCOM Command Support Group offices, directorates, divisions, and branches establish organizational e-mail accounts down to the Command Support Group lowest practical level and in the directorates as far as branch level (two-digit – TCJX-XX) to replace or supplement official memorandums, messages, orders, tasking, or letters. Typically, these messages provide formal direction or establish a formal position, commitment, or response for the organization.

2.7.2. USTRANSCOM organizational e-mail accounts use USTRANSCOM standard organizational abbreviations and office symbols as the User ID and display name (i.e., USTCJ1, USTCJ2, USTCJA, etc.). The standard naming convention for all organizational e-mail accounts begins with “USTC”, including those not directly tied to a specific directorate or Command Support Group.

2.7.3. Essential to doing electronic business is the monitoring of these organizational e-mail boxes. Each office with an organizational e-mail account will designate at least one individual to monitor the organization’s mailbox regularly to ensure messages requiring action are acted upon promptly.

2.7.4. Rules of decorum and format apply to organizational e-mail as if it were a telephone call, message, letter, or other form of communication. Include a formal signature block on all organizational e-mail. Recommend using Times New Roman or Arial style font, black in color, and at least 12 points in size to facilitate viewing from a laptop computer screen.

2.8. Command-Wide Mailers.

2.8.1 Mailers are e-mails sent to large distribution groups and permissions to use these address lists are very limited. *USTC-All* is an address group that includes all command personnel and the following guidelines apply for using this list:

2.8.2. Information provided in the mailer must be relevant to the majority of the command. Other distribution lists are available for smaller user communities (i.e., *USTC-USMC All-Lst*, *USTC-USN All-Lst*, *USTC-J6 All-Lst*). Use SharePoint announcements to share routine information.

2.8.3. *USTC-All* mailers are released through TCCS except for the following individuals and offices: TCCC, TCDC, TCCC-E, TCJ6, DDOC-Chiefs, and USTCJ6-GCCC.

2.9. Individual E-mail.

2.9.1. Individual e-mail accounts are provided to USTRANSCOM personnel to supplement telephone calls, notes, or work-related communications among individuals. Such messages do not generally commit or direct an organization.

2.9.2. Contractor e-mail accounts. Individual accounts for employees of DOD contractors will be provided, if required by the contract. DOD contractors and their employees are authorized use of DOD electronic resources only to the extent necessary to execute contract requirements, unless otherwise provided in the contract or approved by the Contracting Officer. DOD contractors and their employees will be briefed, by their government Contracting Officer Representative, on the policy contained in this instruction prior to being given access to DOD electronic resources. Authorized users who are contractors shall always have their affiliation displayed as part of their e-mail address.

2.9.3. Naming conventions for USTRANSCOM e-mail accounts.

2.9.3.1. USTRANSCOM unclassified e-mail accounts use the standard syntax First.Last@ustranscom.mil. In the Global Address List (GAL), USTRANSCOM military and civilian personnel are identified with the standard display name “Last, First Rank USTRANSCOM JX.” JECC military and civilian personnel are identified with the standard display name “Last, First Rank USTRANSCOM JECC/JX or Last, First Rank USTRANSCOM JECC/JPSE.”

2.9.3.2. USTRANSCOM classified e-mail accounts use the standard syntax “First.Last@ustranscom.smil.mil.” In the classified GAL, USTRANSCOM military and civilian personnel are identified with the standard display name “Last, First Rank USTRANSCOM JX.” JECC military and civilian personnel are identified with the standard display name “Last, First Rank USTRANSCOM JECC/JX or Last, First Rank USTRANSCOM JECC/JPSE.”

2.9.3.3. Civilian Contractors. To help prevent inadvertent disclosure of controlled information, all contractors are identified by the inclusion of the abbreviation "ctr". The standard syntax is “First.Last.ctr@ustranscom.mil” for unclassified accounts and “First.Last.ctr@ustranscom.smil.mil” for classified accounts. Contractor personnel are identified in the GAL by the display name “Last, First CTR USTRANSCOM JX.”

2.9.3.4. Foreign Nationals. When Foreign Nationals are assigned and authorized access to e-mail, the 2-letter English country names and codes specified in ISO 3166 will be used (e.g., John.Smith.uk@ustranscom.mil or John.Smith.uk@ustranscom.smil.mil).

2.10. Safeguard classified and sensitive information at all times. Apply safeguards so information is accessed only on a need-to-know basis by authorized persons, is used only for its intended purpose, retains its content integrity, and is marked properly as required by DODM 5200.01 Vol 2, *Information Security Program: Marking of Classified Information*.

2.11. E-mail is subject to the provisions of the Freedom of Information Act and the Privacy Act of 1974.

2.12. The Federal Records Act requires agencies to identify and preserve records, including records created or received on e-mail systems. E-mail messages are records when they meet both of the following conditions: (a) they are made or received by an agency of the United States Government under federal law or in connection with the transaction of agency business; and (b) they are preserved, or are appropriate for preservation, as evidence of the agency’s or organization’s activities, or because of the value of the information they contain. Disposal of any records, including e-mail, that have been requested under the Freedom of Information Act or in connection with ongoing or imminent litigation, audit, or investigation may need to be frozen or held in suspense until all actions are resolved. The retention period of records is addressed in USTRANSCOM Instruction 33-32.

2.13. Mailbox size limitations allow for the rapid maintenance and recovery of e-mail should a catastrophic event occur. Requests for permanent increases to the command’s default mailbox limit may only be approved by the TCJ6-O or appointed delegate. USTRANSCOM provides

enterprise e-mail archiving capabilities which centralizes administration, increases individual mailbox capacity, and enables remote access to historical e-mail. Personal Folders (.pst files) are only authorized for “read-only” access to legacy e-mail and are not authorized to be stored on networked drives. Flag-Level users will have no storage limit. Other users are restricted to a limit that will be revised from time-to-time.

2.14. Remote access to USTRANSCOM e-mail is permitted via Outlook Web Access from any location that provides internet access; however, common access card (CAC) authentication is required. Therefore, USTRANSCOM members must have a CAC reader and appropriate drivers installed on the system being used to access Outlook Web Access. Division Chiefs or above may authorize the issuance of CAC readers to their members for take-home use. Requests for these devices must come in the form of a signed request letter to TCJ6-OM. Members receiving these devices are solely responsible for the installation of the device on their personal computer. USTRANSCOM will not provide hardware or software support to personal computers to include issues that may result from this installation. Personal computers are defined as any system that was not purchased by USTRANSCOM and configured with USTRANSCOM’s standard image.

2.15. Individuals leaving government service are not authorized to take official records (such as e-mails) with them when they depart. Such an act is considered an improper use of non-public information (see DOD 5500.07-R, *Joint Ethics Regulation*). Individuals who are changing positions within the government and will use the requested information in performing their official duties may request to take their USTRANSCOM e-mail with them when they depart. Contractors are not authorized to take government information, including e-mails, they may have generated or stored on government computer systems.

3. Responsibilities.

3.1. USTRANSCOM Directorate of Command, Control, Communications and Computer Systems (TCJ6), Operations and Plans Division (TCJ6-O), has management responsibility for ensuring the following:

3.1.1. E-mail users within USTRANSCOM are educated and trained on the appropriate use of e-mail according to this instruction and other applicable DOD policies.

3.1.2. Out-processing procedures include removal of accounts for departing personnel within 48 hours of submission for deletion.

3.1.3. Internal storage and control of e-mail is consistent with USTRANSCOM information security and records management policy pursuant to USTRANSCOM Instruction 33-32.

3.1.4. Information assurance, awareness, training, and education are provided to all members.

3.1.5. All members will be notified of their security responsibilities when attempting access to DOD information systems.

3.2. USTRANSCOM Functional Area Communications Computer Systems Managers have responsibility for ensuring the following:

3.2.1 Requests for all personal e-mail accounts are submitted via the Automated Account Request System upon completion of all prerequisite security requirements.

3.2.2. Out-processing procedures include the request for removal of accounts via Automated Account Request System for departing personnel within 24 hours of departure.

3.3. E-mail is a universally accepted, effective, and intuitive tool. These same attributes make it a highly useful medium for all types of malicious activity. E-mail can be used to inject malicious software such as viruses and backdoor programs onto an otherwise secure network. E-mail is also commonly used in phishing or social engineering attacks in which users are enticed to provide information such as passwords, credit card information, or visit a web site that attempts to exploit the user's system. Users must recognize the threats faced when using e-mail and report any unusual activity to the USTRANSCOM Help Desk.

3.3.1. E-mail users shall secure approval from their chain of command before subscribing to or participating in e-mail list servers and newsgroups, except official DOD internal information products.

4. Security.

4.1. Individuals using unclassified DOD automated information systems must have, at a minimum, a National Agency Check or an Entrance National Agency Check in accordance with DOD 5200.2-R, *Personnel Security Program*.

4.2. E-mail administrators must possess a security clearance equal to or greater than the highest security level of the system they administer.

4.3. All individuals will take special care to transmit only that level of classified information for which the system is authorized.

4.4. All individuals will use care when transmitting operational information that if aggregated with other operational information could pose an operations security risk.

4.5. When leaving workstations unattended, individuals will remove their CAC, log out of the system, or lock the workstation.

4.6. Suspected violations of e-mail policy must be reported to either a supervisor, the communications security officer, or an e-mail administrator.

5. Classified E-mail.

5.1. Classified information, up to and including Secret, will be sent over the Secret Internet Protocol Router Network.

5.2. Mark all classified e-mail messages to reflect the highest classification of the information contained in the transmission. Attachments to e-mail should be considered when determining which security classification to put on the message. Mark all paragraphs and subparagraphs with appropriate classification in the same manner as normal correspondence. Reference DODM 5200.01 VOL 2 for additional guidance.

6. Digital Signatures and Encrypted E-mail.

6.1. Digital signatures and e-mail encryption provide an additional layer of security for Sensitive Information. Digital signatures offer positive proof of who sent an e-mail and non-repudiation (prevents denial of transmission) of the e-mail. Encryption prevents unauthorized modification or access to an e-mail during transmission. The CAC is the DOD tool for implementing digital signatures and encryption. A properly configured CAC contains certificates (or keys) that enable users to sign and encrypt unclassified e-mail.

6.2. Digitally encrypting e-mails requires the sender to have the public certificate of the recipient. For USTRANSCOM and many Air Force personnel, this certificate is available in the GAL found in Microsoft Outlook. Certificates for most DOD personnel can be obtained from the Defense Information Systems Agency Global Directory Service at <https://dod411.gds.disa.mil>. For others, prior coordination may be required to obtain the public certificate. This is accomplished by the intended recipient sending a digitally signed e-mail to the sender, who stores the contact information in “Contacts” in Microsoft Outlook. This will allow the sender to digitally encrypt and send an e-mail to the recipient.

6.3. USTRANSCOM E-mail Digital Signature and Encryption Policy. Command personnel will digitally sign all e-mails to provide proof of sender and help combat the effectiveness of “phishing” e-mails. Digital encryption should be used for e-mail containing Sensitive Information as defined in DOD Directive 8500.01E, *Information Assurance*. Encrypting e-mail increases the size of e-mails significantly; therefore, not all e-mail must be encrypted. As a minimum, e-mail pertaining to or alluding to the following topics require the use of encryption in addition to digital signatures prior to transmission:

6.3.1. DOD payroll information.

6.3.2. Logistical data such as requirements, shortages, and shipping information.

6.3.3. Command, control, communications and computer systems outages, shortcomings, or vulnerabilities.

6.3.4. Tasking or support requests.

6.3.5. Financial information such as budgets, funding, and shortfalls.

6.3.6. Resource and procurement management information.

6.3.7. Project-related information such as schedules, timelines, and funding.

6.3.8. Contract-related information.

6.3.9. Contractor proprietary and sensitive/critical data.

6.3.10. Personnel management information.

6.3.11. Orders or other forms of command and control information.

6.3.12. Medical information records under the Health Insurance Portability and Accounting Act (HIPAA).

6.3.13. Account credentials (username and password).

6.3.14. E-mail required to be maintained as “Records.”

6.3.15. Information protected by the Privacy Act.

6.3.16. Documents marked “For Official Use Only.”

6.3.17. Documents marked as “Proprietary.”

6.3.18. Documents marked for “Non-Disclosure.”

6.4. E-mail pertaining to or alluding to the following topics do not require the use of digital encryption prior to transmission:

6.4.1. Non-official correspondence.

6.4.2. Local advertisement of events.

6.4.3. Retirement or promotion invitations.

6.4.4. E-mails of a personal or private nature.

6.4.5. General information for widespread public dissemination

6.4.6. USTRANSCOM mailers.

7. Disclosure Statements. When sending sensitive but unclassified information such as that identified in paragraph 6.3., authors should include a disclosure statement such as those found in Attachment 2.

8. Protection of E-mail Addresses. To reduce the risk of attack on the USTRANSCOM e-mail system, do not indiscriminately release e-mail addresses.

GREGORY E. COUCH
Major General, USA
Chief of Staff

2 Attachments:

1. Glossary of References, Abbreviations, Acronyms, and Terms.
2. E-mail Disclosure Statements.

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

Section A—References

DOD Manual 5200.01 VOL 2, *DOD Information Security Program: Marking of Classified Information*

DOD 5200.2-R, *Personnel Security Program*

DOD 5500-7-R, *Joint Ethics Regulation*

DOD Directive 8500.01E, *Information Assurance*.

USTRANSCOM Instruction 33-32, *Records Management Program*

USTRANSCOM Instruction 33-35, *USTRANSCOM Privacy Act Program*

Section B—Abbreviations and Acronyms

CAC – Common Access Card

DOD – Department of Defense

E-Mail – Electronic Mail

GAL - Global Address List

JECC - Joint Enabling Capabilities Command (including the Joint Planning Support Element and JECC HQ)

USTRANSCOM - United States Transportation Command

Section C—Terms

Not used

Attachment 2

E-MAIL DISCLOSURE STATEMENTS

A2.1. Whenever unclassified, but sensitive information is transmitted electronically, authors should include a “disclosure statement” in the e-mail appropriate for the type of information involved. These statements are designed to advise the reader of: the need to protect the information, the office that may authorized further distribution of the message, and the Freedom of Information Act (FOIA) exemptions that potentially apply. The majority of “disclosure statement” categories used in official USTRANSCOM e-mail communications are listed below. **Do not indiscriminately apply these statements to e-mails; use them only when actually transmitting that type of unclassified, but sensitive information.** Further guidance for management of Privacy Act protected information can be found in USTRANSCOM Instruction 33-35, *Privacy Act Program*. Users can create different “signatures” in Microsoft Outlook for each of the situations below. This will simplify the process of adding the disclosure statements to e-mails.

A2.1.1. Acquisition-related. Use the following statement when sending e-mails that include trade secrets and commercial or financial information obtained from a private non-government source that is privileged/confidential as defined by Exception 4 of the Freedom of Information Act, 5 U.S.C 552 (b)(4).

“FOR OFFICIAL USE ONLY. This electronic transmission may contain trade secrets, or commercial or financial data not intended for disclosure outside government channels and exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C 552. Exemption 4 may apply. Do not further distribute this message without the consent of the originator’s office. If you received this message in error, please notify the sender by reply e-mail and delete all copies of this message.”

A2.1.2. Legal-related. Use the following statement when sending e-mails that include internal records that are deliberative in nature and are part of the decision-making process that contain opinions and recommendations (Exemption 5 of the Freedom of Information Act).

“FOR OFFICIAL USE ONLY. This electronic transmission may contain work-product or information protected under the attorney-client privilege, both of which are protected from disclosure under the Freedom of Information Act, 5 U.S.C 552. Do not release outside of DOD channels without the consent of the originator’s office. If you received this message in error, please notify the sender by reply e-mail and delete all copies of this message.”

A2.1.3. Personal privacy-related. Use the following statement when sending e-mails that include records, which if released, would result in a clearly unwarranted invasion of personal privacy (Exemption 5 of the Freedom of Information Act).

“This electronic transmission may contain FOR OFFICIAL USE ONLY information that must be protected under the Privacy Act of 1974 (see USTRANSCOM Instruction 33.35). Do not release outside of DOD changes without the consent of the originator’s office. If you

received this message in error, please notify the sender by reply e-mail and delete all copies of this message.”

A2.1.4. Medical-related. Use the following statement when sending e-mails that include information obtained from personal medical records.

“This electronic transmission may contain personal medical information protected by the Privacy Act of 1974 (see USTRANSCOM Instruction 33.35) and the Health Insurance Portability and Accountability Act (HIPAA) (see DOD 6025.18-R) and not intended for disclosure outside government channels and exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C 552. Exemption 6 may apply. Do not release outside of DOD channels without the consent of the originator’s office. If you received this message in error, please notify the sender by reply e-mail and delete all copies of this message.”

A2.1.5. Other deliberative process-related. Use the following statement when sending e-mails that include internal records that are deliberative in nature and are part of the decision-making process that contain opinions and recommendations (Exemption 5 of the Freedom of Information Act).

“FOR OFFICIAL USE ONLY. This electronic transmission contains internal matters that are deliberative in nature and/or are part of the agency decision-making process, both of which are protected from disclosure under the Freedom of Information Act, 5 U.S.C 552. Do not release outside of DOD channels without advance approval from the sender. If you received this message in error, please notify the sender by reply e-mail and delete all copies of this message.”

A2.2. The above examples represent the most common types of FOIA-related communication across the DOD. For additional reference to the 48 classes of information specifically protected from disclosure by a federal statute, reference the following web link:
<http://www.defenselink.mil/pubs/foi/>.